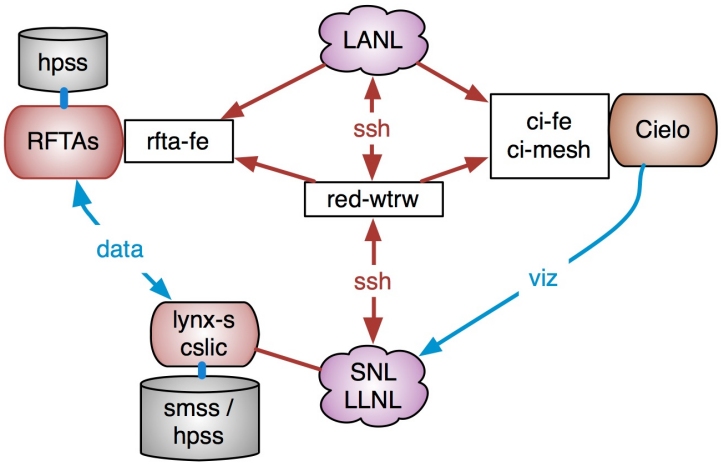
Secure Network Tri-Lab User Access

- Add new comment
- 515 reads

In the Red (ie. Secure Restricted, classified, closed) Network, the three NNSA ASC Laboratories (SNL, LLNL, and LANL) have established a high speed Wide Area Network (WAN) through the DisCom project. This allows logins and file transfers at reasonable speeds between the Red Network gateways such as CSLIC at LLNL, File Transfer Agents (FTAs) at LANL, and Redsky at SNL.

NOTE: there is no equivalent WAN in the **open** network (Unclassified Protected, or Yellow network). Logins and file transfers between systems such as Dawndev at LLNL and Cielito at LANL must go through both Laboratory firewalls and across the Internet using standard tools such as ssh and scp within a VPN session.

You can find HPC documentation and information for LLNL and SNL with a common URL: http://hpc.*site*.gov, where "site" is one of llnl, sandia, or lanl. Here are the links to Livermore, and to Sandia. Also, the main documentation page for computing at Livermore is here: https://computing.llnl.gov/.



Logging-in from LANL to LLNL (such as Sequoia or CSLIC)

Be sure to examine the LLNL Instructions for accessing the LLNL HPC platforms.

1. **Get a Kerberos Ticket**. In order to reach LLNL, you must have a valid LANL kerberos ticket with a LANL IP address, **and** an active account at LLNL (see the Getting an Account web page to obtain one). Typically, you will start from our gateway system in the ICN because of filesystem access. Our gateway is `red-wtrw.lanl.gov`. This gateway will allow a direct `ssh` into the LLNL gateway, the CSLIC cluster, or into Sequoia.

   Upon logging-in to `red-wtrw` via `ssh`, you will already have a kerberos ticket forwarded from your desktop. If you run into problems, ensure your ticket has the correct properties -- that it is *forwardable* from your originating server (ie. workstation). Issue the `klist -f` command on your workstation to see the list of flags in your ticket. They must include the uppercase `F` flag, looking something like this:
   `Flags: FfHAT`
   This ticket is also referred to as your *credential*. If you do not see the uppercase F flag, you can renew your ticket with a `klist -f` command on your workstation and try again. Provide a passcode from your LANL CryptoCard when it prompts you.

   Note: kerberos tickets expire, so verify that the date range of your ticket is valid.

2. **Connect to LLNL**. From the LANL ICN gateway node use the `ssh` command: `ssh -l LLNLmoniker seq.llnl.gov`. If you wish to reach platforms other than Sequoia that do not allow a direct login, you should first connect to `cslic.llnl.gov`, their gateway node.

   - This connects correctly to the LLNL gateway system, CSLIC, but does not necessarily forward your kerberos ticket to LLNL. You might need to obtain a new ticket there after logging-in, but you can check flags with the `klist -f` command.

   - Note that you must provide your LLNL moniker (username) with the `ssh -l` option (lower case L) if it is not the same as your LANL moniker.

   - If you want X11 forwarding into the remote system, you will need to use the *double-hop* method:
     `ssh -X -t red-wtrw ssh -l LLNLmoniker seq.llnl.gov`
     This allows you to run Xwindow commands such as TotalView, xemacs, xterm, etc. and display them back to your desktop.

   Alternative: From some workstations, you can use your fully qualified LANL

moniker to reach Sequoia with your secure LANL Cryptocard:

```
ssh -l LANLmoniker@lanl.gov seq.llnl.gov
```

This will ask you for a passcode, and you can provide one with your secure LANL Cryptocard.

3. (Optional) If you need to acquire a kerberos ticket on a LLNL CSLIC node (to reach Sequoia or elsewhere), issue the
`kinit -f LANLmoniker@lanl.gov`
command. Use your LANL cryptocard when requested.

4. From the LLNL CSLIC gateway, and with a forwardable kerberos ticket, you can log-in to Sequoia directly:
`ssh seq`
and you should get right in.

Logging-in from LANL to SNL's redsky-s

1. **Get a Kerberos Ticket**. First obtain a valid kerberos ticket in your LANL shell session. To reach Redsky, you must have a valid kerberos ticket from your origination point, usually your workstation. You can issue the `kinit -f` command to obtain one. Provide a passcode from your CryptoCard when it asks for a password.
Note: kerberos tickets expire, so verify that you have a valid ticket with the `klist -f` command.

   From there you can `ssh` into the LANL gateway node, `red-wtrw.lanl.gov`.

2. **Connect to SNL**. On the gateway node, issue this command:
`ssh [-l SNLmoniker | -l LANLmoniker@lanl.gov] redsky-s.sandia.gov`
In this command, use either your LANL moniker qualified by the LANL domain for the argument to the -l (lower case L) option, or use your Sandia moniker.
Note: since Redsky is running ssh protocol 2, your kerberos ticket should forward with no problems.

3. (Optional) If you want X11 forwarding into the remote system, you will need to use the *double-hop* method:
`ssh -X -t red-wtrw ssh -l SNLmoniker redsky-s.sandia.gov`

This allows you to run Xwindow commands such as TotalView, xemacs, xterm, etc. and display them back to your desktop.

Logging-in from LLNL or SNL into the LANL HPC Network

If you access Classified LANL HPCs from outside the LANL network, `ssh` to our gateway node, `red-wtrw.lanl.gov`.

1. Log-in to one of your local gateways that provides Red (ie. Classified, Secure Restricted) Network intersite access. At this writing, we know that Sandia's lynx-s and redsky-s and the LLNL CLIC systems all provide connectivity to LANL.

2. **Get a Kerberos ticket**. On your local gateway, issue the `kinit -f` command to obtain a forwardable kerberos ticket. You can check its forwardability with a `klist -f` command to verify it has an uppercase `F` among the `Flags:` field. Authenticate with your local method, cryptocard or SecurID.

3. **Connect to LANL**. From your local gateway, issue this command: `ssh -l` *`LANLmoniker`* `red-wtrw.lanl.gov`.

4. **Connect to LANL HPC cluster**. Now on the LANL `red-wtrw`, (or from anywhere within the LANL Red network), use `ssh` to reach an HPC front-end node. You should be placed into a shell on that front-end. This includes the LANL FTA front-end, `rfta-fe.lanl.gov`.

   The Red Network HPC front-end nodes[1] are (all with .lanl.gov domain):

Red (SRD) Front-end / Compile nodes (accessible via `red-wtrw.lanl.gov`)	
Cielo	`ci-fe`
File Transfer Agents (FTAs)	`rfta-fe`

Luna	`lu-fe`
Typhoon	`ty-fe`
[1]Most HPC clusters have multiple, numbered front-end nodes, but we recommend access through these generic names in this table. This allows wtrw to load-balance in a round-robin fashion.	

5. **SHORTCUT**: You can use the `ssh -t` option to perform the login in a single hop. Also, this is the most convenient (and possibly only) way to open an X11 window (eg. TotalView) for displaying back to your tty using the `ssh -X` command line option. Sample syntax:

   ```
   ssh -t -X red-wtrw.lanl.gov ssh ci-fe3.lanl.gov
   ```

File Transfer

One of the important capabilities for Tri-Lab access of the ASC clusters is file transfer in-between the sites and Laboratories. We have written several scripts to simplify parallel transfers to/from the secure Tri-Lab HPC clusters across the Wide Area Network (WAN). This is a secure encrypted network supporting high bandwidth between the individual ASC machines (CSLIC, Sequoia, Redsky-s, FTAs, HPSS, SMSS, etc.). You can use special scripts to transfer files over the secure DisCom WAN; here is how:

1. External users at Sandia or LLNL must first reach the LANL gateway. LANL users can skip this step if originating from a LANL workstation:
   `ssh -l LANLmoniker red-wtrw.lanl.gov`

2. The LANL File Transfer Agents (FTAs) provide file transfer services. First log-in to the FTA front end node:
   `ssh rfta-fe`

3. On the FTA front-end node, request a file-transfer node from Moab (or multiple nodes for large parallel transfers):
    - Batch: `msub scriptname`
    - Interactive: `msub -I -l nodes=nodecount`
4. Use the parallel ftp (`pftp`) or the `hsi2` command scripts in /usr/projects/packages /datools/fta/bin. You can see them with an
`ls /usr/projects/packages/datools/fta/bin/pftp*`
command. These two commands ship files to specific systems (Sandia's SMSS, LLNL HPSS, etc.). As an example, here is the command for transferring a file to the LLNL HPSS:
`pftp2llnl filename`
These commands are configured to use the high-speed WAN and to transfer in parallel based on the number of nodes your job requested from Moab.